**Cybersecurity** is the process of protecting information by preventing, detecting, and responding to attacks.

Threats can be categorized as events that can affect the confidentiality, integrity, or availability of the organization’s assets. These threats can result in destruction, disclosure, modification, corruption of data, or denial of service.

Examples of the types of threats an organization can face include the following

* Natural disasters
* Hacker attacks
* Cyberattack
* Viruses and malware
* Disclosure of confidential information
* Denial of service (DOS/DDOS) : an attack against availability

**Threat actors**: individual or group of individuals who performs an attack or are responsible for a security incident that impacts or has the potential of impacting an organization or individual

They are several types of threat actors:

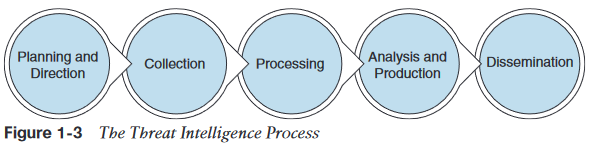
* **Script kiddies**: People who use existing scripts or tool to hack into computers and networks
* **Organized crime groups**: Their main purpose is to steal information, scam people, and make money
* **State sponsors and governments**
* **Hacktivists**
* **Terrorist group**

**Hackers Categories**

* **White hat hackers**: these individuals perform ethical hacking to help secure companies and organizations
* **Black hat hackers**: these individuals perform illegal activities, such as organized crime
* **Gray hat hackers**: these individual usually follow the law but sometimes venture over to the darker side of black hat hacking

Threat Intelligence Process

Security intelligence, threat intelligence : tool in preventing cyber attacks



**Viruses and worms**

**Virus**: need a host program or file to infect. They require some type of human interaction.

**Worm**: can travel from to system without human interaction

**Transmission methods**

* Master boot record
* BIOS infection
* File infection
* Macro infection
* Cluster
* Multipartite

**Trojans**

Programs that pretend to do one thing but, when loaded, actually performs another, more malicious act.

A software Trojan horse is based on this same concept. A user might think that a file looks harmless and is safe to run, but after the file is executed, it delivers a malicious payload

The payload is executed if the attacker can get the victim to open the file or click the attachment. That payload might allow a hacker remote access to your system, start a keystroke logger to record your every keystroke, plant a backdoor on your system, cause a denial of service (DoS), or even disable your antivirus protection or software firewall.  
Unlike a virus or worm, Trojans cannot spread themselves. They rely on the uninformed user.

**Trojan types:**

**Remote access trojans (RATs):** allow the attacker full control over the  
system. Remote-access Trojans are usually set up as client/server programs so that the attacker can connect to the infected system and control it remotely

**Data hiding:** The idea behind this type of Trojan is to hide a user’s data. This type of malware is also sometimes known as ransomware. This type of Trojan restricts access to the computer system that it infects, and it demands a ransom paid to the creator of the malware for the restriction to be removed

**E-banking:** These Trojans intercept and use a victim’s banking information for financial gain

**Denial of service (DoS)**: These Trojans are designed to cause a DoS

**FTP**: These Trojans are specifically designed to work on port 21. They allow the  
hacker or others to upload, download, or move files at will on the victim’s machine.

**Security-software disablers**: These Trojans are designed to attack and kill antivirus  
or software firewalls.

**Proxy:** These Trojans are designed to work as proxy programs that help a hacker hide and allow him to perform activities from the victim’s computer, not his own.

**Trojan goal:**

Credit card data, electronic or digital wallets, passwords, insider information, data storage, advanced persistent threat APT

**Trojan infection Mechanisms:**

Peer-to-peer network, Instant messaging, Internet Relay Chat , email attachments, physical access, browser and browser extension vulnerabilities, sms messages, Impersonated mobile apps, watering hole, freeware

**Injection vulnerabilities**

They are many software and hardware vulnerabilities: SQL injection vulnerabilities, HTML injection vulnerabilities, command injection vulnerabilities

An attacker takes advantage of code injection vulnerabilities to inject code into a vulnerable system and change the course of execution.

**SQL Injection vulnerabilities**: They can allow an attacker to view, insert, delete, or modify records in a database.

In SQL injection attack, the attacker inserts or injects partial or complete SQL queries via the web application. The attacker injects SQL commands into field in an application or a URL in order to execute predefined SQL commands.

**SQL injection categories:**

**In band SQL**: the attacker obtains the data by using the same channel that is used to inject the SQL code. The data is dumped directly in web application or web page.

**Out-of-band SQL**: the attacker retrieve data using a different channel (email, instant message … can be used)

**Blind SQL:** the attacker does not make the application display or transfer any data; rather, the attacker is able to reconstruct the information by sending specific statements and discerning the behavior of the application and database.

To perform an SQL injection attack, an attacker must craft a syntactically correct SQL statement (query)

**HTML Injection**: injection is a vulnerability that occurs when an unauthorized user is able to control an input point and able to inject arbitrary HTML code into a web application.  
Successful exploitation could lead to disclosure of a user’s session cookies; an attacker might do this to impersonate a victim or to modify the web page or application content seen by the victims.

**Command injection**: attack in which an attacker tries to execute command that he is not supposed to be able to execute on a system via a vulnerable application

Session Hijacking

Predicting session tokens

Session sniffing: This can occur through collecting packets if unencrypted web

Main in the middle attack: the attacker sits in the path between the client and the web server.

Man in the browser attack: similar to main in the middle attack; but a browser is compromised and used to intercept and manipulate web sessions between the user and the web.

Default credentials

Attackers can easily identify and access systems that use shared default password

Insecure Direct Object Reference Vulnerabilities: They can be exploited when applications allow direct access to objects based on user input. An attacker can modify the value of a parameter used to directly point to an object

Cross-site Scripting (XSS): web applications vulnerabilities

XSS categories:

Reflected XSS: ex : a user being persuaded to follow a malicious link to a vulnerable server that injects the malicious code back to user’s browser

Stored XSS: This attack occurs when the malicious code or script is permanently stored on a vulnerable or malicious server, using a database.

Ex: a user requesting the stored information from vulnerable or malicious server, which causes the injection of the requested malicious into the victim’s browser.

DOM based XSS: cross-platform and language-independent application programming interface that treats an HTML, XHTML, or XML document as a tree structure.

In DOM based XSS attacks, the attacker sends a malicious URL to the victims, and after the victims clicks on the link, it may load a malicious website or a site that has a vulnerable DOM route handler

Cross-site Request forgery (CSRF) attacks: occur when unauthorized commands are transmitted from a user who is trusted by the application. This attack exploits the trust that an application has in a user’s browser.

Cookie Manipulation attacks: it is possible when vulnerable applications store user input and then embed that input in a response within a part of the DOM.

Race conditions:

Unprotected APIs

Confidentiality: requirement that private or confidential information not be disclosed to unauthorized individuals

Concepts of confidentiality:

* Identifying what information should be controlled
* Identifying who is not authorized to access information
* Controlling access to the information so that only authorized parties can access it

Encryption: is a one of the most common ways to protect the confidentiality of a system or its data

Some sensitive data: (social security numbers, bank and credit card account information, patient and health records, military secrets…)

Examples of security mechanisms designed to preserve confidentiality:

Logical and physical access controls, encryption, database views, controlled traffic routing

Integrity: is a requirement that information and programs are changed only in a specified and authorized manner

Availability: applications and data must be available to authorized users when they needed and requested

Access Control Management: security features that govern how users and processes communicate and interact with systems and resources.

Authentication credentials: Three categories of factors:

Knowledge (something the user knows, possession (something a user has), inherence (something the user is)

Cloud security Threats

Clouds advantages: distributed storage, scalability, resource pooling, access from any location, measured service, automated management

Clouds deployment models:

* Public cloud: open for public
* Private cloud: used just by the client organization on the premises or at a dedicated area in a cloud provider.
* Community cloud shared between several organizations
* Hybrid cloud: composed of two or more clouds

Cloud computing basic models: IaaS, PaaS, SaaS

Cloud computing security :

IOT protocols

Zigbee: takes advantage of the underlying security services provided by the IEEE 802.15.4 Mac layer. The 802.15.4 Mac layer supports the AES algorithm with a 128 bit key for both encryption and decryption

Bluetooth Low Energy (BLE) and Bluetooth Smart

Z-Wave